e-dea NETWORKS | CYBER SECURITY

BOLETÍN INFORMATIVO

17 - julio – 2026

622 Vulnerabilidades de Microsoft - Patch Tuesday

Microsoft publicó la actualización de seguridad más grande registrada con un número de 622 vulnerabilidades corregidas, incluidas dos zero-day explotadas activamente y una divulgada públicamente.

Entre las vulnerabilidades se encuentra CVE-2026-56155, una elevación de privilegios en Active Directory Federation Services (AD FS), y CVE-2026-56164, una falla de elevación de privilegios en Microsoft SharePoint Server que puede ser explotada de forma remota sin autenticación. Microsoft también corrigió CVE-2026-50661, una vulnerabilidad de omisión de BitLocker que había sido divulgada.

Microsoft publicó 154 actualizaciones de seguridad durante julio de 2026, mitigando un total de 622 CVE's.

Estás actualizaciones incluye diversos productos clave como Windows, Office, Edge, SharePoint, SQL Server, Azure, Exchange, Defender y Visual Studio.

Productos **afectados**

Familia de Productos	Cantidad de CVE
Windows	**416**
Microsoft Office	**82**
Microsoft Defender	**5**
Herramientas para desarrolladores	**27**
Microsoft Edge	**46**

Familia de Productos	Cantidad de CVE
SharePoint Server	**17**
Azure	**11**
SQL Server	**8**
Servidor Exchange	**5**
Otros productos de Microsoft	**5**

Vulnerabilidades críticas

Algunas de las vulnerabilidades críticas más importantes son:

- ***CVE-2026-48561*** *– Ejecución remota de código en Microsoft Copilot*
- ***CVE-2026-49164*** *– ejecución remota de código en Active Directory Domain Services*
- ***CVE-2026-54999*** *– Ejecución remota de código en Windows TCP/IP*
- ***CVE-2026-54992*** *– Ejecución remota de código en Windows Message Queuing (MSMQ)*
- ***CVE-2026-48564*** *– Ejecución remota de código del servicio de servidor DHCP*
- ***CVE-2026-54117 y CVE-2026-54118*** *– Ejecución remota de código en Microsoft SQL Server*
- ***CVE-2026-50522 y CVE-2026-58644 –*** *Ejecución remota de código en Microsoft SharePoint*
- ***CVE-2026-55011 y CVE-2026-55012 –*** *Ejecución remota de código en Microsoft Defender*
- ***CVE-2026-58608 –*** *Ejecución remota de código en Windows Print Spooler*
- ***CVE-2026-49796 –*** *Ejecución remota de código de Windows GDI+*
- ***CVE-2026-50694*** *– Ejecución remota de código en Windows Secure Socket Tunneling Protocol (SSTP)*
- ***CVE-2026-54982 y CVE-2026-54995*** *– Ejecución remota de código en el controlador Windows Reliable Multicast Transport Driver (RMCAST)*

Vulnerabilidades de día cero

CVE	Producto	Impacto	Estado
CVE-2026-50661	Windows BitLocker	Omisión de funciones de seguridad	CONOCIDA PÚBLICAMENTE
CVE-2026-56155	Servicios de federación de Active Directory	Elevación de privilegios	EXPLOTADA ACTIVAMENTE
CVE-2026-56164	Microsoft SharePoint Server	Elevación de privilegios	EXPLOTADA ACTIVAMENTE

Versiones afectadas: *Windows 10, Windows 11 y Windows server 2016, 2019, 2022 y 2025.*

Severidad: **Crítica**

Recomendaciones

Parches

Actualizar a las versiones corregidas indicadas por el fabricante y validar la documentación.
***NO** intentar aplicar todo a la vez. La estrategia clave es la priorización basada en la exposición y el riesgo, no en la cantidad de CVEs.*

Configuración

Si utilizas SharePoint Server 2016 o 2019, ten en cuenta que han llegado al final de su soporte extendido; considera la migración como remediación.

Microsoft recomienda habilitar la integración de AMSI (Antimalware Scan Interface) en el servidor y configurar el modo de Request Body Scan en "Full". Esto ayuda a detectar cargas útiles maliciosas en el cuerpo de la solicitud incluso antes de que el parche este aplicado.

Fuentes: Release note - Microsoft,